Synopsis for Registration as Research Student

For

Doctoral Degree

on

“Some issues on architecture for secure services for IoT”

By

BaseshankarAbhishek Abhimanyu

Research Scholar

Supervisor

Dr. Yashwant V. Joshi

Department of Electronics and Telecommunication Engineering

Shri Guru GobindSinghji Institute of Engineering and Technology,

Nanded-431606. (MS.) India.

Abstract: Smart city infrastructure is forming a large scale IoT system with widely used IoT devices that generate huge amount of data. Cloud supported IoT has been broadly deployed in smart cities. Recently a new infrastructure has been proposed i.e. fog computing, which is to be integrated with IoT to enabling computer services devices deployed at network edge. The fog computing can provide faster response and greater quality of service for IoT applications. In fog computing security is the important issue, so in this work there will be focus on the various security issues occurring during the data flow from lower layer to upper layer of the system. In this work the main objective is to provide the security to the data generated at the node. As there is no standard architecture designed for Fog based IoT infrastructure, so in this work firstly the drawbacks in the existing architecture is found and the new architecture is proposed which will be highly secured while improving the bandwidth and delay issues.

Introduction: The internet of things (IoT) is projected to have a huge impact on the life of human beings. Report shows the huge increase in the number of devices per person, i.e. more than 6 devices per person on an average by year 2020.This mainly devoted to price reduction of the devices which makes them more accessible for everyone.

IoT is a multilayer architecture, divide into the four layer as perception layer, networking layer, service layer and application layer [1].

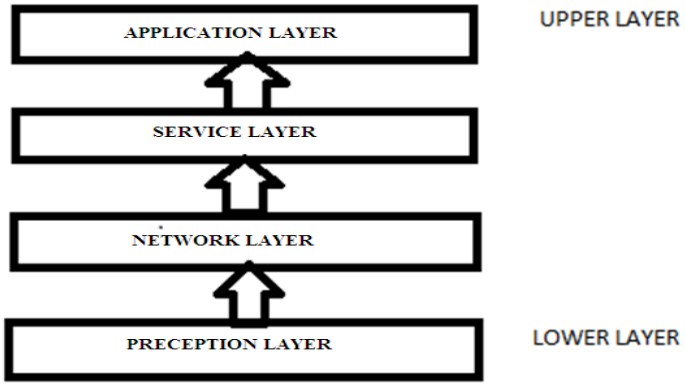

Fig.1. Layer Architecture of IoT

As shown from the figure 1 the perception layer is the bottom layer of IoT model which is also known as sensor layer. This layer interact with physical devices and components through smart devices (such as RFID, sensors, actuators etc).The layer above the perception layer is the network layer which is also known as transmission layer. This layer is used to receive processed information provided by perception layer and determine the routes to transmit the data and information. Next layer is the service layer which provides efficient and secure services to objects or application. The top layer in IoT architecture is application layer which is also known as business layer. The application layer receives the data transmitted from network layer and uses the data to provide required services or operations.

In the past, most of the existing IoT platforms, are built only based on cloud platform. However this is no longer a sustainable and economical model for next generation of IoT smart city platform where it requires ultra-low latency and fast response time. Recently there is a new trend to offload more computation from the cloud and device layer to the middle layer component which are IoT gateways and edge networks called fog computing. The fog computing is infrastructure organized by the networking edge devices or clients to provide computing services for customers or applications in space between network central server and end users. In fog computing, the massive data generated by different IoT devices can be

processed at the network edge instead of transmitting it to the centralized cloud infrastructure due to bandwidth and latency concern.

Since fog computing based architecture is organized as distributed architecture and can processes and store data in network edge devices[3], which is close to the end user can provide services with faster response and greater quality in comparison with cloud computing. In fog infrastructure, a number of fog nodes are connected, if fog node does not have enough resources to provide the request services from nearby end user while its neighboring nodes have spare resources, the fog node can move some local data to its neighboring nodes to be processed and store data. Hence all the fog nodes have to be connected with each other,which will arises the issue of security, hence to solve the security issues the data generated at the perception layer have to be encrypted before applying to the higher layers.

Literature survey:

The Jie Lin et al. [1] has proposed the fog based infrastructure for IoT to enable computing services devices deployed at network edge, aiming to improve the user's experience and resilience of the services in case of failures. With the advantage of distributed architecture and close to end-users, fog/edge computing can provide faster response and greater quality of service for IoT applications. Thus, fog/edge computing-based IoT becomes future infrastructure on IoT development. In this work, authors conduct a comprehensive overview of IoT with respect to system architecture, enabling technologies, security and privacy issues, and present the integration of fog/edge computing and IoT, and applications. Particularly, this paper first explores the relationship between cyber-physical systems and IoT, both of which play important roles in realizing an intelligent cyber-physical world. Authors relate IoT architecture with the cyber physical system and they have concluded that the IoT is the horizontal architecture which connects the communication layer of all the cyber physical system.

Then, existing architectures, enabling technologies, and security and privacy issues in IoT are presented to enhance the understanding of the state of the art IoT development. To investigate the fog/edge computing-based IoT, this paper also investigates the relationship between IoT and fog/edge computing, and discuss issues in fog/edge computing-based IoT.

Authors have also purpose the four layer IoT architecture which designed for fog infrastructure. In this work authors have discuss the security associated with the IoT architecture. The resource allocation among all the fog nodes because of lack of resources in the edge nodes was found to be key problem. Finally, several applications, including the smart grid, smart transportation, and smart cities, are presented to demonstrate how fog/edge computing-based IoT to be implemented in real-world applications.

The white paper by Atmel [2] has discussed about the security issues for IoT. In this the existing internet security technologies such as SSL and TLS, were also discussed along with critical issue occurs in the network when the edge node will be accesses by the advisory. In this the various benefits available to the nodes whose identity has been verified are outline. This paper has mention the various types attracts occur in the edge node. Finally they have given the smart solution to the encryption for the edge node thereby using crypto accelerator devices.

Bin Cheng et al. [3] has proposes a standard-based approach to design and implement a new fog computing based framework, namely FogFlow, for IoT smart city platforms. They have also discuss about how to dynamically configure and manage data processing tasks over cloud and edges and how to optimize task allocation for minimal latency and bandwidth consumption. In addition, they have compare the exiting fog computing framework while designing their propose framework; This FogFlow programming model allows IoT services developers to perform elastic IoT services easily over cloud and edges also it supports standard interfaces to share and reuse contextual data across services. In this work they have also discus three different case studies namely, Anomaly detection of energy consumption, Video surveillance in stadiums and Smart city Magnifier. Travis Mick, Reza Tourani, Satyajayant Misra proposes lightweight authentication and secured routing (LASeR) for NDN(Named Data Networking IoT in Smart Cities[4], a secure on boarding and routing framework for) NDN- based IoT network. In this work Scalability is achieved through a hierarchical network design, and very little cryptographic or computational burden.

Federico Montoriononi proposed an architecture [5] open to extensions in several ways and still allowing the coexistence of diverse data gathering methods.

Joshua E. Siegel et al. propose a solution modeled [6] on human use of context and cognition, leveraging cloud resources to facilitate IoT on constrained devices. They present an architecture applying process knowledge to provide security through abstraction and privacy through remote data fusion. They outline five architectural elements and consider the key concepts of the “Data Proxy” and the “Cognitive Layer.” The Data Proxy uses system models to digitally mirror objects with minimal input data, while the Cognitive Layer applies these models to monitor the system’s evolution and to simulate the impact of commands prior to execution. The Data Proxy allows a system’s sensors to be sampled to meet a specified “Quality of Data” (QoD) target with minimal resource use. The efficiency improvement of this architecture is shown with an example vehicle tracking application. Finally, they consider future opportunities for this architecture to reduce technical, economic, and sentiment barriers to the adoption of the IoT.

Zhitao Guan et al. [7] proposed a secure and efficient data acquisition scheme for Cloud-IoT in smart grid. In the proposed scheme, the large data is partitioned into several blocks, and the blocks are encrypted/decrypted and transmitted in sequence. In addition, they adopt the dual secret sharing scheme, which realizes the privacy-preserving, the data integrity check and the attributes check simultaneously. The analysis shows that the proposed scheme can

meet the security requirements of data acquisition in smart grid, and it also reduces response time overhead significantly compared to other popular schemes.

The white paper by XILINX [8] examines three key applications areas that comprise the foundation of IoT connectivity, cyber security, and edge compute within the context of selecting an IoT edge platform that can adapt to the impact of market trends over time.

Identified Research Problems:

- Many researchers are working to discover various issues and challenges related to design and architecture of IoT. Since IoT devices are connected to the cloud/fog, so there is a need of designing and testing higher end protocols and standards in order to support each and every individual layers of IoT.
- In future, number of devices connected to the internet will be increasing in huge number. So a special concern will be dedicated to the security of IoT, since all devices will be interconnected with each other.
- Traditional security mechanisms are deployed at the Internet edge. Those mechanisms were used to protect the network from external attacks. Such mechanisms are no longer enough to secure the next generation Internet.

Problem Definition:

- Study and identify the short comings in the existing Architecture of Internet of Things.
- Analyze different methods and methodology to satisfy various requirements in Internet of Things for different applications.
- Propose new design of secure architectures for IoT applications.
- Develop an application based on proposed architecture to get real time performance parameter.
- Compare the performance of proposed architectures with exiting architectures.

Probable Solution:

- Design the Framework to secure the IoT environment which will comprise of three layers.

Authentication

At the heart of this framework is the authentication layer, used to provide and verify the identify information of an IoT entity. When connected IoT devices (e.g., embedded sensors and actuators or endpoints) need access to the IoT infrastructure, the trust relationship is initiated based on the identity of the device. The way to store and present identity information may be substantially different for the IoT devices. Note that in typical enterprise networks, the endpoints may be identified by a human credential (e.g., username and password, token or biometrics).

Authorization

The second layer of this framework is authorization that controls a device's access throughout the network fabric. This layer builds upon the core authentication layer by leveraging the identity information of an entity. With authentication and authorization components, a trust relationship is established between IoT devices to exchange appropriate information.

Network Enforced Policy

This layer encompasses all elements that route and transport endpoint traffic securely over the infrastructure, whether control, management or actual data traffic. Like the Authorization layer, there are already established protocols and mechanisms to secure the network infrastructure and affect policy that are well suited to the IoT use cases.

- Encrypt the data generated by the lower layers using hardware crypto accelerators, such crypto accelerators provides keys, stored in well-hidden, protected hardware that ensures that the keys will never be visible in the way they would be, if advisory tries to do the same calculations in software or in unprotected hardware.

- Design IoT Security Framework based on Artificial Intelligence concepts:

  Swarm intelligence (SI) is a technological area, which can inspire the design of new IoT security solutions. A subfield of artificial intelligence, SI studies the emergent collective intelligence of groups of agents based on social behavior that can be observed in nature, such as ant colonies, flocks of birds, fish schools and bee hives, where number of individuals with limited capabilities are able to produce intelligent solutions for complex problems. Vulnerability and reaction to threats seem to be a common thread and IoT can take inspiration from ant colony, flocks of birds, fish schools and bee hives on how to react on threats.

  Tools Used:

  a)**EXata**

  EXata uses a software virtual network (SVN) to digitally represent entire networks, including the various protocol layers, antennas, and devices.

  With this, the system can interoperate, at one or more protocol layers, with Real radios and devices to provide hardware-in-the-loop capabilities. EXata can also be connected to systems with real applications, which run on the SVN just as they would run on real networks. 67 EXata mimics the functions of a real network so that it appears, interacts, and behaves like the real network. This provides an exact, reproduction of external behavior so that the emulated system is indistinguishable from the real one.

  b) Cooja

  Cooja is an emulator built over the Contiki OS. Contiki OS is a tiny OS which is optimized to be used with very little memory footprint and minimal processing capabilities. It is specially designed to be used for Internet of things. It can also emulate nearby peer to peer communication among the nodes and nearby broadcast of messages based on distance. It emulates all the functionalities by building over the abstraction layer of contiki OS. Since it emulates over a real OS it can do time based profiling

of different functions. However, as it is built over contiki OS, all the nodes in the network are simulated to be running the same tiny OS.

c) NS3

NS3 is the Network Simulator 3 which is the open-source, research-oriented, community supported simulator for testing networking protocols. It supports almost all communication protocols such as MQTT, ZigBee, and Bluetooth etc. It also supports different modules which allows parallel simulation, distributed simulation etc. It can be extended easily to support and test different applications.

d) **OMNeT++**

OMNeT++ is discrete event-based simulator which is written in C++ and is used for simulation of communication networks, distributed systems and other multiprocessor applications [13]. It is a generic simulator which allows the development of various simulation models and frameworks on top of it.

f) **MATLAB**

MATLAB products offer support collecting IoT data and analyzing it in the cloud. One option for storing data as prototype of IoT system is the ThingsSpeak IoT analytic platform, which collects data from connected things. The ThingsSpeak web service provides API and an MQTT broker for posting or publishing data. If data will be collected in Thing Speak, user can use react and time control features of Thing Speak to execute MATLAB code based on characteristics of data or based on a fixed time schedule. If data is already stored in a database, on a private cloud, or in another IoT platform that has a web API, it can be access from MATLAB using Database Toolbox or built-in web services commands provided by MATLAB. Database Toolbox allows user to access data stored in any ODBC-compliant and JDBC-compliant databases using SQL commands.

References:

[1] Lin Jie, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, and Wei Zhao. "A survey on internet of things: Architecture enabling technologies security and privacy and applications." *IEEE Internet of Things Journal,* March2017, Volume:4, pp.2327-4662.

[2]Atmel-8994-Security-for-Intelligent-Connected-IoT-Edge-Nodes.2015 Atmel Corporation. /Rev.:Atmel-8994A-CryptoAuth-Security-for-Intelligent-Connected-IoT-Edge-Nodes-WhitePaper_112015.

[3] Cheng Bin, Gürkan Solmaz, Flavio Cirillo, Ernö Kovacs, Kazuyuki Terasawa, and Atsushi Kitazawa. "FogFlow: Easy Programming of IoT Services Over Cloud and Edges for Smart Cities." *IEEE Internet of Things Journal*, August 2017, Volume:2, pp.2327-4662.

[4] Mick Travis, Reza Tourani, and Satyajayant Misra. "LASeR: Lightweight Authentication and Secured Routing for NDN IoT in Smart Cities." *IEEE Internet of Things Journal*, July 2017, pp.2327-4662.

[5] Montori, Federico, Luca Bedogni, and Luciano Bononi. "A Collaborative Internet of Things Architecture for Smart Cities and Environmental Monitoring." *IEEE Internet of Things Journal*, June 2017, Volume:4, pp. 2327-4662.

[6] Siegel, Joshua E, Sumeet Kumar, and Sanjay E. Sarma. "The Future Internet of Things: Secure, Efficient, and Model-Based*." IEEE Internet of Things Journal*, October 2017, pp. 2327-4662.

[7] Guan, Zhitao, Jing Li, Longfei Wu, Yue Zhang, Jun Wu, and Xiaojiang Du. "Achieving Efficient and Secure Data Acquisition for Cloud-Supported Internet of Things in Smart Grid" *IEEE Internet of Things Journal*, April 2017, Volume: 4, pp.2327-4662

[8] Chetan Khona. " Key Attributes of an Intelligent IIoT Edge Platform." White Paper: All Programmable Devices XILINX. WP493 (v1.0) September 6, 2017.

[9] Ni, Jianbing, Kuan Zhang, Xiaodong Lin, and Xuemin Shen. "Securing fog computing for internet of things applications: Challenges and solutions." *IEEE Communications Surveys & Tutorials*, October 2017, Volume: 20, pp.1553-877X.

[10] Dr. Ovidiu Vermesan, and Dr.Peter Friess, eds. *Internet of things converging technologies for smart environments and integrated ecosystems.* River Publishers, 2016.

[11] https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html,CISCO 2017, Accesses Date 25/03/2018.

[12] Huadong Ma, Liang Liu, Anfu Zhou, and Dong Zhao "On Networking of Internet of Things: Explorations and Challenges" *IEEE Internet of Things journal*, October 2015, Volume: 3, Aug. 2016, pp.2327-4662

Research Scholar **Guide**

Abhishek Baseshankar **Dr. Yashwant.V Joshi**